4-

allowance of the application is respectfully requested.

After re-analyzing the Secure4U publication, the applicant respectfully submits that Secure4U actually presents a different solution than the present invention because of the following reasons:

a. The concept of <u>learning the normal behavior</u> of an application has not been implemented nor suggested by Secure4U.

b. The concept of the <u>learning period</u> also has not been implemented nor suggested by Secure4U.

c. The solution presented by Secure4U deals only with Web browsers, probably since the implemented technology (which is not disclosed in said publication of Secure4U) suits only to Web applications. However, the present application deals with a generic problem, which may be implemented not only to web browsers, but to any other application.

d. The term "sandbox" is used by Secure4U as follows: "Secure4U creates <u>a close environment (sandbox) around your web browser</u> to restrict access to any of your computer's resources." However, the term "sandbox" is used by the present invention as the analog of the enforcement file, i.e. as analog to the definition of normal / abnormal behavior: "The general operation of this embodiment is as shown in Figure 1 which is a flow diagram showing how an embodiment may be installed on a computer 10, may be manually activated 12, or may automatically be led to detect installed software 14 and may see that <u>the details of the enforcement file, or sandbox,</u> are adhered to 16. At the next computer boot 18 the embodiment returns to the detection step 14."

Moreover, the specification of the present application comprises a detailed description upon which a person of ordinary skill in the art may implement the invention. For example, the illustration and description of Fig. 4. However, the publication of Secure4U does not disclose any technical information upon which a person of ordinary skill in the art may implement it, but merely the result of the solution.

Therefore, the present claims are deemed patentable over Secure4U, and favorable reconsideration thereof is respectfully requested.

Claim 19 stand rejected under 35 U.S.C 103(a) as being unpatentable over Rose (5,144,660) in view of Shane (5,793,972).

The applicant respectfully submits that although both the present invention and Rose direct to protecting against malicious elements, e.g. Trojans and viruses, their purpose still differs. While Rose directs to "... protecting a <u>computer</u> ..." (Rose, the abstract), the present invention "... relates to controlling <u>application software</u> ..." (The present invention, Field of the invention). Thus, while Rose directs to protecting <u>physical elements of the computer</u>, the present invention relates to protecting <u>logical elements of the computer</u> (i.e. application programs).

While Rose discloses a <u>hardware</u> solution to the monitoring and enforcement issues, the present invention presents a <u>software</u> solution to these issues. According to Rose "The device monitors the disk drive 14 of the computer. The device monitors the bus ..." (Rose, the abstract). But the present invention does not deal with the <u>hardware</u> aspect of the disk drive or the bus, but with <u>software</u>.

The applicant respectfully submits that in the present application the term "learning period" refers to a period where there is a reasonable certainty that the application is not infected by a virus. For example, assuming that a program was legally purchased, at the first period after the installation of the program on the user's machine there is a high certainty that the application is not infected by a virus. During this period the accesses of the application to data storage locations (files, folders, etc.) are registered (referred in the present application to as "enforcement file"), and after this period is over, they will be considered as the normal behavior of the program. After the learning period ends, any access to files will be tested over the registration, and accesses that do not correspond to the normal behavior will be considered and treated as suspected.

Thus, the terms "learning" and "learning period" do not refer by the present application to the "number of acceptable unauthorized attempts within a

predetermined period of time" as stated in section 6 of the outstanding Office Action.

The following description of the present application refers to the learning issue: "... the system allows the attempt and learns the details so that in future an access to that area of the disk will always be allowed. Thus a specific enforcement file is gradually built up over the duration of the learn mode." (The present application, page 9 lines 15 to 17).

The Examiner's rejection is based on the combination of Rose and Shane. As pointed out by the Examiner, Rose is completely silent regarding the gradual building of an enforcement file during a period of time, such that information about accessing elements of data storage that have been carried out during said period is stored within said enforcement file. However, the Examiner's position was that the concept of this gradual building during a "learning period" is taught by Shane. The applicant respectfully submits that according to Shane (see Shane column 10, and specifically lines 37 to 45) information about unauthorized accesses are recorded during a given period of time "to determine if an excessive amount of invalid identification codes have been submitted within a pre-determined period of time" (Shane column 6, lines 51 to 53). However, according to the present invention, the protection feature is based on the opposite idea: all accesses attempts made by a program within a given period of time are recorded in an enforcement file and are considered allowable, such that following said period of time attempted access may be compared against said allowable activities.

Moreover, Shane does not deal with any aspect of protection against Trojan, viruses or other malicious executables. Thus the combination of Rose and Shane is not obvious to a person of ordinary skill in the art at the time the invention was made. Furthermore, even when combining Rose with Shane, the result still differs from the present invention.

Therefore, claim 19 is deemed allowable and favorable reconsideration thereof is respectfully requested.

Claim 21 stand rejected for the similar reasons as per claims 19 and 20. Thus, claim 21 deemed allowable and favorable reconsideration thereof is respectfully requested.

Claim 22 stand rejected for the similar reasons as per claims 19 and 20. Thus, claim 21 deemed allowable and favorable reconsideration thereof is respectfully requested.

Claim 24 contains the subject matter of claims 19 and 23, indicated as allowable by the Examiner in the last Office Action.

Applicant has carefully studied the remaining prior art of record herein and concludes that the invention as described and claimed in the present application is neither shown in nor suggested by the cited art.

In view of the foregoing remarks, all of the claims are believed to be in condition for allowance. Favorable reconsideration and allowance of the application is respectfully requested.

Respectfully submitted,

Christopher J. McDonald

Claim 19 (Amended): Apparatus for ensuring the integrity of an application executed on a computer having data storage arranged sectorwise, comprising:

apparatus for learning about the normal behavior of said application by monitoring accesses of said application to elements of said data storage during a limited period; and

an enforcement device, operative after said period is over, for identifying and preventing said application from accessing elements of data storage that do not correspond with the normal behavior of said application.

Claim 24 (new) Apparatus for ensuring the integrity of a computer application to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising:

apparatus for assigning a general enforcement file to each new program;

apparatus for learning about the program by monitoring the program of said data storage, by monitoring the program's attempts to make file accesses during a learning period;

an enforcement device operative, after said learning period is over, to treat attempts of the program to access files accessed during said learning period more leniently than attempts of the program to access files not accessed during said learning period; said enforcement device is based at least on instances of specific permission being given by the user to said application to access locations of said data storage, wherein said enforcement device treats attempts of said application to access locations of said data storage to which the user has permitted to access during said learning period more leniently than attempts of the program to access files to which the user did not permit access during said learning period.

Claim 25 (new): A method for detecting abnormal behavior of a first application executed on a computer system, and preventing the damage thereupon, comprising:

- monitoring accesses of said application to elements of data storage over a period of time and storing information about said accesses in an enforcement file, thereby learning the normal behavior of said application;
- when said period is over, detecting attempts of said application to access elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon.

Claim 26 (new): A method according to claim 25, further comprising enabling the user of said first application to determine said normal behavior during said learning period.

Claim 27 (new): A method according to claim 25, further comprising enabling the user of said first application to determine said normal behavior after said learning period is over.

Claim 28 (new): A method according to claim 26, further comprising enabling the user of said first application to determine said normal behavior after said learning period is over.

Claim 29 (new): A method according to claim 25, further comprising detecting attempts of a daughter application of said first application to access elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon.

Claim 30 (new): A method according to claim 26, further comprising detecting attempts of a daughter application of said first application to

access elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon.

Claim 31 (new): A method according to claim 27, further comprising detecting attempts of a daughter application of said first application to access elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon.

Claim 32 (new): A method according to claim 25, further comprising detecting attempts of a second application to access elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon.

Claim 33 (new): A method according to claim 26, further comprising detecting attempts of a second application to access elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon.

Claim 34 (new): A method according to claim 27, further comprising detecting attempts of a second application to access elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon.

Cont
B7

<u>Claim 35</u> (new): A method according to claim 29, wherein said second application is executed on a second computer.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: GRUPER

Serial No.   : 08/937,883

Filed   : 9/25/97

For   : SOFTWARE APPLICATION ENVIRONMENT

Group Art Unit: 2783

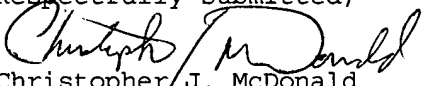Examiner: J. Follansbee

Hon. Commissioner of Patents and Trademarks

Washington, D.C. 20231

Sir:

Attached is a marked up copy of claim 19 to be included with the Request for Continued Examination filed on Sept. 16, 2002

Respectfully submitted,

Christopher J. McDonald
Reg. 41,533

19.(amended)   Apparatus for ensuring the integrity of [computer applications to be run in association with] an application executed on a computer having data storage arranged sectorwise [in a storage device], comprising:

[apparatus for assigning a general enforcement file to each new program;]

apparatus for learning about [the program] the normal behavior of said application by monitoring [the program's attempts to make file accesses during a learning period] accesses of said application to elements of said data storage during a limited period; and

an enforcement device operative, after said [learning] period is over, [to treat attempts of the program to access files accessed during said learning period more leniently than attempts of the program to access files not accessed during said learning period] for identifying and preventing said application from accessing elements of data storage that do not correspond with the normal behavior of said application.